OTRS Spotlight: Corporate Security 2024

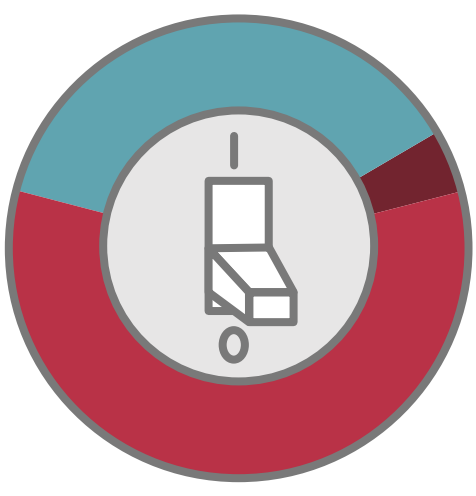
Teil 1: Die Folgen des CrowdStrike-Vorfalls

93 %

Nach dem CrowdStrike-Vorfall haben 93 % der befragten Unternehmen ihre Sicherheitsvorkehrungen erhöht.

- **45 %** haben ihre IT- und Software-Landschaft diversifiziert, um weniger abhängig von einzelnen Software-Anbietern zu sein.
- **40 %** haben erweiterte Echtzeit-Überwachungs- und Warnsysteme eingeführt.
- **39 %** haben zusätzliche Tests für neue Patches und Updates eingeführt.
- **39 %** haben einen Incident Response Plan eingeführt oder ihren bestehenden aktualisiert.
- **36 %** haben Disaster Recovery und Backup-Pläne implementiert oder bestehende aktualisiert.
- **26 %** sind zu stufen-/phasenweisen Rollouts von Patches und Updates übergegangen.
- **24 %** haben Unified Endpoint Management (UEM) eingeführt.
- **17 %** haben automatische Updates für all ihre Software deaktiviert.
- **4 %** haben keine Maßnahmen ergriffen und **3 %** wissen es nicht.

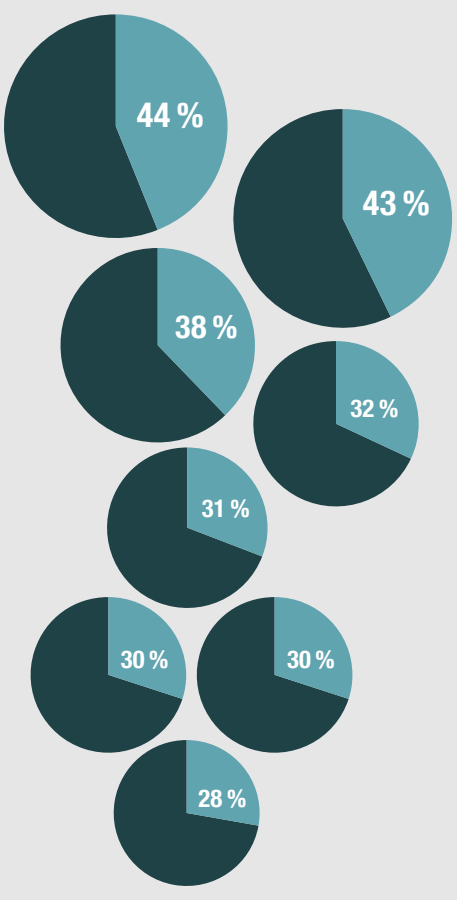
Auch wenn nicht alle Unternehmen direkt vom CrowdStrike-Vorfall betroffen waren, war er für die meisten ein Weckruf, ihre IT-Sicherheit zu verbessern.



Waren Systeme in Ihrem Unternehmen von dem IT-Ausfall betroffen, der durch das von CrowdStrike im Juli 2024 ausgerollte fehlerhafte Update verursacht wurde?

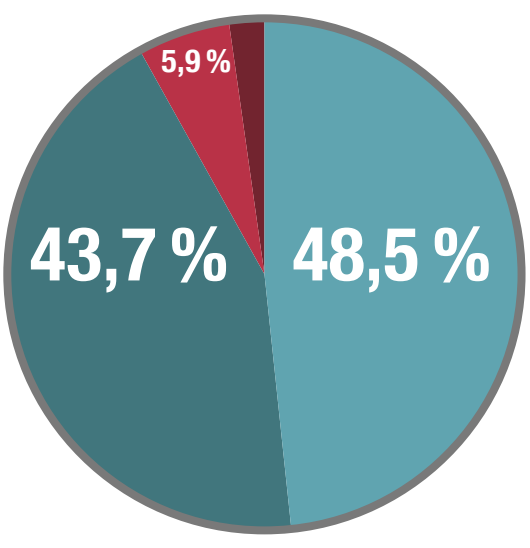
- **58,2 %** Ja.
- **37,4 %** Nein.
- **4,4 %** Ich weiß es nicht.

Nur wenige der direkt Betroffenen waren darauf vorbereitet, die Auswirkungen des CrowdStrike-Vorfalls mit eigenen Ressourcen einzudämmen.



- **44 %** ergriffen die **von CrowdStrike beschriebenen Maßnahmen zur Behebung des Problems**, sobald diese verfügbar waren.
- **43 %** installierten den **von CrowdStrike bereitgestellten Fix**, sobald dieser verfügbar war.
- **38 %** verwenden **erweiterte Echtzeit-Monitoring- und Warnsysteme**, die es ihnen ermöglicht haben, schnell einzugreifen.
- **32 %** verfügen über robuste **Rollback-Mechanismen, Disaster Recovery und Backups**, sodass sie ihre Systeme schnell wieder auf eine stabile Version zurücksetzen konnten.
- **31 %** verwenden **Unified Endpoint Management (UEM)**, wodurch sie betroffene Systeme schnell identifizieren und Maßnahmen zur Eindämmung der Auswirkungen (remote) einleiten konnten.
- **30 %** verfügen über einen **robusten Incident Response Plan**, der ihnen half, das Problem schnell zu identifizieren, zu isolieren und zu beheben.
- **30 %** führen bei neuen Patches und Updates grundsätzlich **Tests vor der Bereitstellung** durch, wodurch sie den Defekt erkennen und schnell eingreifen konnten.
- **28 %** führen grundsätzlich **stufen-/phasenweise Rollouts** durch, so dass nur wenige Systeme von dem Vorfall betroffen waren.

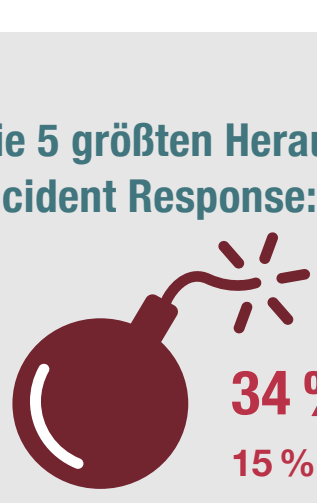
Ein gefundenes Fressen für Angreifer: Die Hälfte aller Security-Teams hält ihre Organisation nicht für optimal auf Sicherheitsvorfälle vorbereitet.



Wie gut ist Ihr Unternehmen auf Sicherheitsvorfälle vorbereitet?

- **48,5 %** Optimal.
- **43,7 %** Akzeptabel.
- **5,9 %** Nicht ausreichend.
- **1,9 %** Ich weiß es nicht.

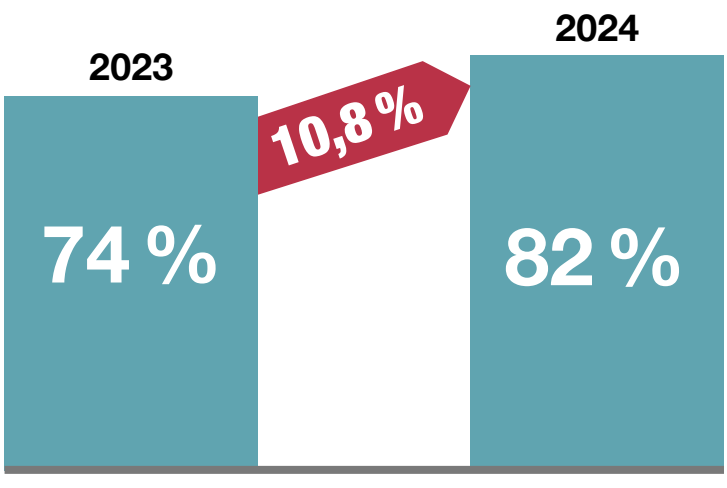
Die 5 größten Herausforderungen für Security-Teams bei der Incident Response:



34 % Sich schnell entwickelnde Bedrohungen

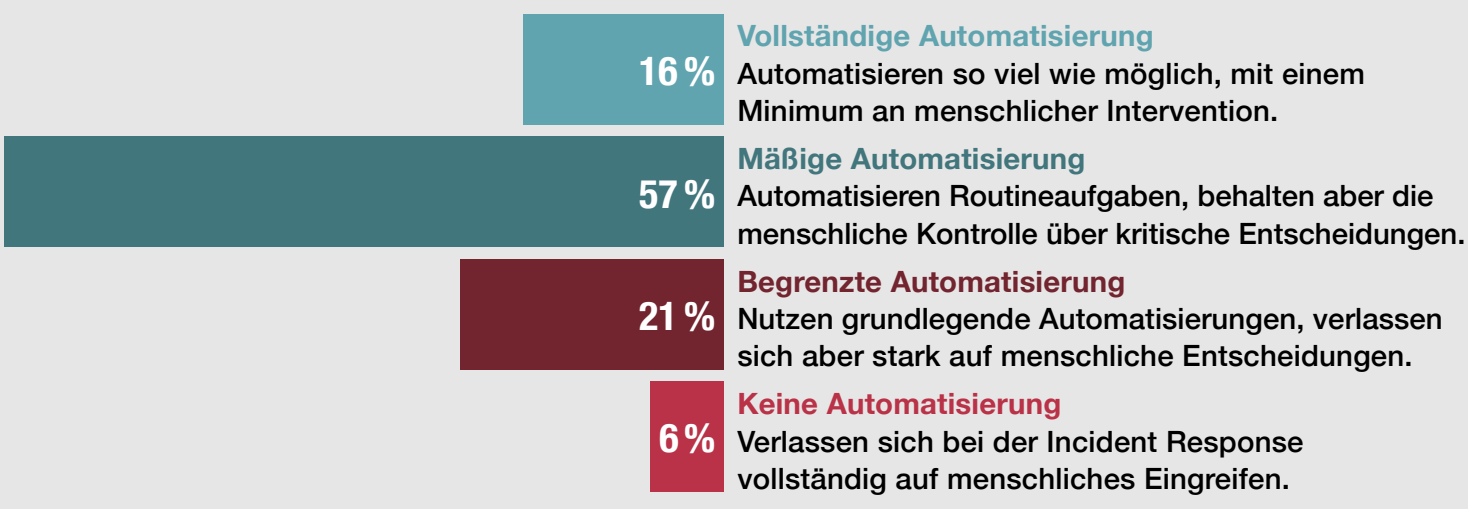
- **15 %** Durchführung umfassender Post-Incident Reviews
- **12 %** Mangel an qualifiziertem Personal
- **12 %** Rechtzeitige und angemessene Kommunikation mit der Öffentlichkeit
- **12 %** Mangelnde Integration zwischen Tools

Die Zahl der Sicherheitsvorfälle nimmt jedes Jahr zu, sodass es für Security-Teams schwierig ist, mit den Angreifern mitzuhalten.



„Ja, wir haben einen Anstieg von Sicherheitsvorfällen registriert."

Indem sie ihre Incident Response-Prozesse automatisieren, können Security-Teams besser mit den sich schnell verändernden Bedrohungen Schritt halten.



Die verwendeten Daten beruhen auf einer Online-Umfrage der Pollfish Inc. im Auftrag der OTRS AG, an der 476 IT- und Cybersecurity-Fachkräfte in Deutschland, USA, Brasilien, Mexiko, Australien und Malaysia zwischen dem 22.08. und 17.09.2024 teilnahmen. Sofern nicht anders angegeben, beziehen sich alle Zahlen auf den Durchschnitt aller untersuchten Länder.

OTRS